UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,449	06/10/2005	Pim T Tuyls	NL02 1343 US	3797

65913 7590 07/08/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
07/08/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/538,449	TUYLS ET AL.	
	Examiner	Art Unit	
	Sarah Su	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☒ Claim(s) *1,4-9,11,15-17,20 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/10/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Preliminary Amendment, received on 10 June 2005, has been entered into record. In this amendment, claims 1, 4-9 and 11-24 have been amended.

2. Claims 1-26 are presented for examination.

Priority

3. The claim for priority from PCT/IB03/05335 filed on 21 November 2003 is duly noted.

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

5. The information disclosure statement filed 10 June 2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Specification

6. The abstract of the disclosure does not commence on a separate sheet in accordance with 37 CFR 1.52(b)(4). A new abstract of the disclosure is required and must be presented on a separate sheet, apart from any other text.

7. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

Claim Objections

8. Claims 1, 4, 11, 15-17, 20 and 24 are objected to because of the following informalities:

a. Claims 1 and 17 do not contain proper transitional phrases. See MPEP § 2111.03.

b. In claim 4, line 5: "the value x" lacks antecedent basis;

c. In claim 4, line 9: "the value y" lacks antecedent basis;

d. In claim 11, line 5: "the value x" lacks antecedent basis;

e. In claim 11, line 10: "the value y" lacks antecedent basis;

f. In claim 14, line 4: "squareof r" should read –square of r–;

g. In claims 14 and 16, line 5: "a verifier device" is unclear if it relates to "a verifier device" (claim 14, line 3);

h. In claim 20, line 8: "a verifier device" is unclear if it relates to "a verifier device" (claim 20, line 2);

i. In claim 24, the claim does not have the proper claim identifier. See 37 CFR 1.121(c).

Appropriate correction is required.

Drawings

9. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 21 (Figure 2) and 302, 303 (Figure 3).

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "31" has been used to designate both a processor in a verifier device (page 10, lines 6-7) and a processor in a trusted third party device (page 10, lines 9-10).

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being

amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 25-26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. These claims are omnibus type claims.

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-3 are rejected under 35 U.S.C. 101 because the claimed invention lacks patentable utility. Claims 1-3 are directed toward a method of verifying the knowledge of a secret number s. The claims are directed to a judicial exception; as such, pursuant to the Interim Guidelines on Patent Eligible Subject Matter (MPEP 2106)), the claims must have either physical transformation and/or a useful, concrete

and tangible result. The claims fail to include transformation from one physical state to another. Although, the claims appear useful and concrete, there does not appear to be a tangible result claimed. Merely verifying would not appear to be sufficient to constitute a tangible result, since the outcome of the verifying step has not been used in a disclosed practical application nor made available in such a manner that its usefulness in a disclosed practical application can be realized. As such, the subject matter of the claims is not patent eligible.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-3, 10-12, 14-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Naccache (EP 0578059 A1).

As to claims 1, 14, 17, Naccache discloses a method for executing number-theoretic cryptographic and/or error-correcting protocols, the method having:

> **verifying the knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein** (page 4, line 1-5).

As to claim 2, Naccache discloses:

the zero knowledge protocol is the Fiat-Shamir protocol (page 3, lines 4-5).

As to claim 3, Naccache discloses:

the zero knowledge protocol is the Guillou-Quisquater protocol (page 4, lines 15, 33-34).

As to claims 18 and 21, Naccache discloses:

(i) providing to the verifier device a value $v=s^2$ being the Montgomery multiplication of the secret number s (i.e. B) **by itself** (page 4, lines 16-17);

(ii) computing, by the prover device, the value $x = r \times_m r$, where r is a random number and transmitting the value of x (i.e. T) **to the verifier device** (page 4, line 19);

(iii) selecting, by the verifier device, a challenge value of e (i.e. d) **from the set {0, 1} and transmitting the challenge value to the prover device** (page 4, line 21);

(iv) computing, by the prover device, the value $y = r \times_m s^e$ and transmitting the value y (i.e. U) **to the verifier device** (page 4, line 23);

(v) the verifier device checking the authenticity of the prover's response according to the values of *x, y* and *v* previously received and according to the challenge value *e* (page 4, lines 25-28).

As to claim 10, Naccache discloses:

all computations in the zero knowledge protocol are performed using Montgomery representation of numbers and using Montgomery multiplication operations (page 4, lines 1-5).

As to claims 11, 19, 20 and 22, Naccache discloses:

(i) providing to the verifier device a value s^e being the Montgomery e^{th} (i.e. d) **power of the secret number s** (i.e. B) (page 5, line 28);

(ii) computing, by the prover device, the value $x=r^e$, being the Montgomery e^{th} (i.e. d) **power of r** (i.e. D) **where r is a random number, and transmitting the value of x to the verifier device** (page 5, line 28);

(iii) selecting, by the verifier device, a challenge value of c (i.e. e) **from the set {0, 1, . . . e-1} and transmitting the challenge value to the prover device** (page 6, line 8);

(iv) computing, by the prover device, the value $y = r \times_m s^c$ and transmitting the value y (i.e. U) **to the verifier device** (page 4, line 23);

(v) the verifier device checking the authenticity of the prover's response according to the values of x, y and s^e previously received according to the challenge value c (page 6, lines 12-14).

As to claim 12, Naccache discloses:

wherein the step of checking the authenticity of the prover's response comprises the step of computing the values of y^e and $x \times_m s^{ec}$ and checking that they are the same (page 6, lines 12-14).

As to claim 15, Naccache discloses:

means for selecting a random number, r (i.e. R) (page 3, line 20);

means for computing the Montgomery square of r to obtain x (page 3, line 20);

means for transmitting x (i.e. Z) **to a verifier device** (page 3, lines 20-21);

means for receiving a challenge value, e (page 3, line 23);

means for computing the Montgomery product of $y = r \times_m s$ (page 3, lines 25-30);

means for transmitting y to the verifier device (page 3, line 25).

As to claim 16, Naccache discloses:

means for selecting a random number, r (i.e. R) (page 3, line 20);

means for computing the Montgomery e^{th} power of r to obtain x (page 5, line 28);

means for transmitting x to a verifier device (page 5, line 28);

means for receiving a challenge value, c (i.e. e) (page 6, line 8);

means for computing the Montgomery product of $y = r \times_m s$ (page 3, lines 25-30);

means for transmitting y to the verifier device (page 4, line 23).

As to claims 23 and 24, Naccache discloses:

a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of claim 1 (page 3, lines 54-57).

As to claim 25, Naccache discloses:

Apparatus substantially as described herein with reference to the accompanying drawings (page 3, lines 54-57).

As to claim 26, Naccache discloses:

A method substantially as described herein with reference to the accompanying drawings (page 4, lines 1-5).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

18. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache as applied to claim 11 above, and further in view of Brickell (US Patent 7,165,181 B2).

As to claim 13, Naccache does not disclose:

repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Naccache, as evidenced by Brickell. Brickell discloses a system and method for establishing trust without revealing identity, the system and method having:

repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover device (col. 6, lines 29-30).

Given the teaching of Brickell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Naccache with the teachings of Brickell by repeating the authorization procedure. Brickell recites motivation by disclosing that repeating the procedure makes it less likely that an unauthorized or cheating prover can succeed in providing adequate proof to a challenger (col. 6, lines 66-67; col. 7, lines 1-3). It is obvious that the teachings of Brickell would have improved the teachings of Naccache by repeating the authentication procedure in order to prevent a cheating prover from successfully providing correct information to a challenger.

Allowable Subject Matter

19. Claims 4-9 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Prior Art Made of Record

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Gilbert et al. (US Patent 5,987,138) discloses a system and method for an identification and/or signature process.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131